DEPARTMENT OF DEFENSE

ANNUAL STATEMENT OF ASSURANCE

FISCAL YEAR 2000

VOLUME I

VOLUME I
TABLE OF CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY AND INTRODUCTION

The Department of Defense (DoD) Annual Statement of Assurance is produced in two volumes. Volume I is a synopsis of the most significant internal management control problems (DoD systemic control weaknesses) and the corrective measures underway to resolve those weaknesses. Volume II is a detailed analysis of specific DoD Component internal management control weaknesses that have no clear correlation to the systemic weaknesses. DoD Component weaknesses, however, are considered significant by the management of those DoD Components that have reported them.

The requirements of Section 4 of the Federal Managers' Financial Integrity Act (FMFIA), are satisfied in the Department's "Financial Management Improvement Plan" (FMIP). The National Defense Authorization Act of 1998 directed the Department to produce the FMIP on a biennial basis; however, the Department has chosen to publish the FMIP on an annual basis. The FMIP addresses financial management within the Department, including the feeder systems not owned or controlled by the DoD financial community that provide data to the Department's accounting and finance systems. Since the FMIP addresses critical aspects of DoD financial management operations, it covers many of the financial reporting requirements specified in other laws and regulatory legislation. It is structured as a single integrated document that incorporates all germane regulations and, consequently, satisfies the requirements of the FMFIA, section 4. Both the DoD FMIP, dated January 2001, and the DoD FY 2000 Annual Statement of Assurance will be available on the Internet at http://www.dtic.mil/comptroller/.

The Fiscal Year 2000 DoD Statement of Assurance reports the assurance statements submitted by the DoD Component heads in the prior Administration. Those statements reflect existing conditions within the Department at that time. While, under previous Administrations, the focus of the Statement of Assurance process has been on identifying management control weaknesses and the corresponding remedial action plans, we plan to modify that approach by placing added emphasis on improving controls and integrating required corrective actions into the Department's annual program and budget review process. In addition, we will emphasize the use of meaningful performance metrics to improve evaluation of progress made in resolving all management control problems.

The Fiscal Year 2000 DoD Statement of Assurance has identified six overall systemic weaknesses. Although they closely parallel those reported in past DoD Annual Statements of Assurance, there are several changes both in the content of these weaknesses as well as in some of the milestones associated with the weaknesses. The "Unreliable Financial Reporting of Personal and Real Property" systemic weakness, previously reported as a separate weakness, has been incorporated into the "Financial Management Processes and Systems" systemic weakness in this year's report. This change treats property valuation reporting the same as other valuation reporting weaknesses encompassed within the "Financial Management Processes and Systems" systemic weakness. Additionally, one weakness that was reported last year--"Acquisition Process and Systems"--has been closed out. The unresolved systemic weaknesses for FY 2000 are:

1. Financial Management Processes and Systems

2. Total Asset Visibility

3. Management of Unexploded Ordnance

4. Information Assurance

5. Year 2000 Computer Problem

6. Personnel Security Investigations Program

The overall operational effectiveness of the Department and its ability to provide assurance that it is able to achieve its mission objectives--currently and in the long-run--are the focus of Volume I. This volume provides an overview of the systemic concerns identified by DoD senior management, as well as related concerns raised by the federal central agencies. Volume I also summarizes the fundamental logic being employed to resolve these concerns and provides assurance that DoD internal controls adequately support the accomplishment of mission objectives.

DOD STATEMENT OF REASONABLE ASSURANCE

As required by the Federal Managers' Financial Integrity Act (FMFIA), this Annual Statement of Assurance, in its entirety, addresses the management controls of the Department and makes disclosures required by the FMFIA. With the exception of the disclosed weaknesses, the Department has reasonable assurance that its internal controls are effective in fulfilling its mission and policy responsibilities.

This conclusion is predicated on findings from evaluations conducted as part of the Department's implementation of the FMFIA (the DoD Management Control Program) and DoD senior management assessment of other information pertaining to the effectiveness of management controls. Although this Annual Statement of Assurance reports weaknesses in some management controls, the control weaknesses are not of sufficient materiality to endanger the Department's ability to accomplish its national security responsibilities.

The methods and procedures in place serve as effective safeguards to assure the Department's effective stewardship of its resources. The Department's controls, where deficient, are bolstered by other effective controls and reliable procedures that assure the Department's ability to field forces and provide an appropriate response to actions that impinge on the safety and security of the nation, as directed by the President of the United States.

This Annual Statement of Assurance was crafted consistent with guidance issued by the Secretary of Defense on February 12, 1994, which mandated the participation of the Department's most senior managers in the identification and resolution of DoD-wide systemic control problems. Based on the Secretary's direction, both the Deputy Secretary of Defense and the Under Secretary of Defense (Comptroller) subsequently defined and promulgated the responsibilities of managers with respect to the DoD Management Control Program. The systemic control weaknesses identified in this volume, and actions outlined to resolve those weaknesses, reflect the Department's commitment to address and resolve deficiencies. Volume I disclosures also reflect accomplishments to date.

Financial Management Processes and Systems

Statement of the Problem: The Department categorizes its financial management systems as accounting, finance, and feeder systems. (Within the DoD environment, "feeder systems" are functional systems such as acquisition, inventory management and property management systems that furnish data to DFAS accounting and finance systems.) The Defense Finance and Accounting Service (DFAS) owns and is responsible for most of the Department's accounting and finance systems, whereas the DoD Components (i.e., the Military Services and Defense Agencies) own and are responsible for the Department's feeder systems. The Department's financial management systems, taken as a whole, generally were planned, designed or implemented to satisfy the various financial management statutes and standards that existed at the time but do not meet new requirements that have been mandated and promulgated within the past few years. Therefore, many of the Department's systems currently are not capable of producing financial information that satisfies fully the scrutiny of business-like financial statement audits.

Effective with this report, the "Unreliable Financial Reporting of Personal and Real Property" systemic weakness has been incorporated into the "Financial Management Processes and Systems" weakness. This change treats property valuation the same as other valuation reporting weaknesses encompassed within the "Financial Management Processes and Systems" systemic weakness.

Source of Identification: DoD financial managers as well as reports by the General Accounting Office (GAO); Office of the Inspector General, DoD (OIG,DoD); and DoD Component audit organizations.

Cause and Impact of the Problem: The Department's accounting, finance, and feeder systems do not fully comply with current federal financial management systems requirements. As a result, financial data generated for inclusion in the Department's annual financial statements generally cannot pass new and stringent audit requirements.

Many of the Department's existing accounting, finance, and feeder systems cannot readily be modified to meet new or changing functional requirements imposed in legislative mandates and federal regulations. Adding to the difficulty in upgrading the Department's financial management systems is the complex array of separate systems or subsystems that operate within specific DoD organizational entities or functional areas, but do not always interface electronically with one another. Consequently, the latest technological innovations too often cannot readily be incorporated into these systems. Data common to, or required by, multiple systems cannot always be exchanged among the systems in a timely, effective, or efficient manner. In essence, many systems continue to operate in stand-alone modes rather than in an integrated electronic network. As a result, in certain instances, program and financial managers do not have access to specific financial information in a format that is timely and useful. As a result, the federal audit community and the public, at times, have perceived that the Department does not effectively manage the resources that it has received from the Congress.

Possible Solutions: The Department has undertaken a number of significant initiatives to improve its financial management processes, systems and information. Since its inception in 1991, the DFAS has worked steadily toward ensuring that its accounting and finance systems comply with applicable federal requirements. The DFAS strategy is based upon two primary elements: (1) eliminate or replace noncompliant systems and (2) develop or modify and implement systems that comply with federal financial management systems requirements.

As of September 30, 2000, the Department operated 15 critical finance systems and 61 critical accounting systems. The Department is continuing to eliminate legacy systems to achieve its goal of 37 accounting and finance systems (i.e., 30 operated by the DFAS and 7 operated by other DoD Components) that will comply with federal financial management systems requirements. New systems currently under development or to be developed also will be required to comply with federal requirements.

Providing reliable, consistent and timely financial management information involves all functional communities within the Department, not just the financial management community. Much of the data needed for sound financial reporting comes from feeder systems operated by DoD functional communities other than the DoD financial management community. The feeder systems, such as those that perform logistics, acquisition, personnel, and medical functions, are owned by their respective functional communities. Therefore, much of the effort to improve the Department's financial reporting involves working with those functional communities to upgrade their systems, internal controls and systems interfaces.

As of September 30, 2000, the Department reported 91 critical feeder systems. The DoD Components currently are evaluating these systems to ascertain their compliance with federal financial management systems requirements and accounting standards. Thus far, the Components have reported that 6 of these critical feeder systems have been determined to comply with federal requirements, 23 systems did not comply, and 14 systems had not been fully evaluated. The Components also have indicated that 48 of the reported critical feeder systems are scheduled to be eliminated or replaced.

Annually, the Department prepares and submits to the Congress and the Office of Management and Budget (OMB) a Financial Management Improvement Plan (FMIP). The Plan presents the Department's overall strategic approach to improve its financial management. The Plan includes the Department's financial management concept of operations, which identifies the roles and responsibilities that financial managers, operational commanders, and program managers must perform to substantially enhance financial management within the Department. The Plan also presents information on DoD financial management systems initiatives, including accounting, finance, and feeder systems. Finally, the Plan assists the DoD Components in focusing their efforts to conform with federal and DoD system requirements.

Major Milestones for Corrective Actions (C = Completed)

Date	Milestone
C	Designate the DFAS as the primary project office responsible for the Department's finance and accounting operations, financial management systems development and implementation.
C	Develop the overall concept of systems architecture for migration systems.
C	Determine and obtain Chief Financial Officer approval of significant financial functional requirements.
C	Standardize the accounting classification coding structure and data element definitions.
C	Select migratory/interim migratory finance and accounting systems.
C	Develop an inventory of systems impacted by the "Year 2000 problem;" prepare and execute a plan to implement the Year 2000 systems changes.
C	Reduce, by 50 percent, the outstanding balance of unmatched disbursements and negative unliquidated obligations reported as of June 1993.
C	Establish senior management governing bodies to monitor operations and identify solutions for resolving financial management weaknesses and deficiencies.
C	Improve the Federal Managers' Financial Integrity Act processes.
C	Develop and approve systems implementation schedules.
C	Reduce, clarify, and reissue published policies and procedures through publication of all volumes of the DoD Financial Management Regulation.
C	Publish the initial edition of DFAS' "A Guide to Federal Requirements for Financial Management Systems."
C	Complete consolidation of the DFAS-controlled accounting and finance sites into 5 Centers and no more than 20 Operating Locations.
C	Complete the Year 2000 mission critical systems changes.
C	Develop implementation strategies and supporting milestones for correcting specific major material deficiencies identified by the OMB in its memorandum of June 5, 1998.

Planned Milestones (FY 2001)

C	Implement the "Critical Finance and Feeder System Compliance Process" and recharter the Senior Financial Management Oversight Council to oversee the Process.
6/01	Update, and reissue in the appropriate medium, the DFAS' "A Guide to Federal Requirements for Financial Management Systems to serve as the "set" of requirements for the Systems Compliance Process."
Continuous	Reengineer DoD finance and accounting processes.
Continuous	Resolve, to the maximum extent feasible, unmatched disbursements and negative unliquidated obligations over 180 days old.
Continuous	Implement applicable solutions, in accordance with previously approved Implementation Strategies, to correct material deficiencies identified by the OMB in its letter dated June 5, 1998, and through subsequent audits. (Certain tasks may continue beyond FY 2000.)
Continuous	Implement DFAS' migratory finance and accounting systems.
Continuous	Integrate finance and accounting systems with feeder systems.

Planned Milestones (Beyond FY 2001)

9/02	Continue to resolve significant systems interface/integration issues (i.e., personnel, acquisition, logistics, contracting and property).
9/03	Continue to incorporate appropriate finance, accounting, and feeder systems enhancements.
9/03	Implement additional financial management systems enhancements (as deemed necessary).
10/03	Implement necessary modifications/enhancements of finance, accounting, and feeder systems to better ensure that those systems comply with applicable federal financial management systems requirements..

Office of the Secretary of Defense Functional Proponent Point of Contact:

Mr. Gerald Thomas
Directorate for Business Policy
Office of the Under Secretary of Defense (Comptroller)
Telephone: (703) 604-6350, extension 125

Related Initiatives

Individual DoD Components have reported to the Office of the Under Secretary of Defense (Comptroller) their efforts to correct identified management control weaknesses that impact or are directly related to ongoing initiatives to correct DoD-wide financial management system weaknesses. Those efforts generally are covered in the Department's "Financial Management Improvement Plan" and the recently approved "Financial and Feeder Systems Compliance Process."

Total Asset Visibility

Statement of the Problem: The Department did not have a capability to share logistics information concerning the location, condition, quantity, and availability of assets within and between its Component headquarters and the Commanders-in-Chief (CINCs) of the Unified Commands. The Department needs this capability across the functional areas of supply, transportation, maintenance, medical, procurement and personnel, and throughout all management levels from wholesale through retail. Additionally, the information must be provided to the operational Joint Task Force commanders, as well as logistics and weapons systems managers. The Components have developed their own systems which give them an asset visibility capability within their own respective organizations. Those systems now must be integrated (and any voids identified and fixed) so that the Department may effectively and efficiently manage, deploy, and recover assets to meet critical readiness, contingency, and other requirements.

Source of Identification: Experience during deployment and sustainment of forces in times of war or contingency/emergency operations, as evidenced in Operation Desert Storm and, to a lesser extent, in Rwanda and Haiti.

Potential Impact of the Problem: The problem has an adverse impact on readiness, both during contingencies and other operations, and results in overspending for items of supply. The inability of a unit to "see" where its requisitions are in the pipeline causes that unit to lose confidence in the system when the materiel does not arrive on schedule. As a result, the usual response is to requisition the materiel again. Unfortunately, this duplication typically causes already strapped supply and transportation systems to fall farther behind in efforts to move materiel. The inability to manage and allocate transportation and other logistics assets to the degree required also is a significant problem. Ports of debarkation are severely restricted by lack of information regarding the contents of containers and the ultimate consignees, causing severe backlogs during contingencies. Item Managers, unaware in many cases of "on hand" assets at units, often program and buy additional materiel when such requirements could be satisfied from current assets if they were "visible" to the Item Manager.

Possible Solutions: In September 1994, the Deputy Under Secretary of Defense (Logistics) (DUSD(L)) established a DoD Total Asset Visibility (TAV) Joint Task Force to provide validation, oversight, and direction for a Joint TAV Program, through the development of a universally understood and accepted JTAV Implementation Plan. On April 21, 1995, the DUSD(L) designated the Army as the Executive Agent and established the JTAV Office to lead the initiatives for further development and implementation of the TAV capability to the CINCs, Services, and other DOD organizations.

In November 1995, the Army, as the Executive Agent, published the final version of the JTAV Implementation Plan, which was approved by the Under Secretary of Defense (Acquisition and Technology) and distributed throughout the Department of Defense. In executing the plan, the JTAV Office developed an Operational and Systems Architecture designed to capture, see, share and use logistics data and information across DoD in a timely, useful and secure manner.

On June 1, 1998, the Defense Logistics Agency became the Executive Agent to facilitate integration with on-going automated identification technology efforts. Since that time, the JTAV application to provide logistics information concerning the location, condition, quantity, and availability of assets to the Unified Commands and Components has undergone extensive development and will be completed and moved into the sustainment mode at the end of FY 2000.

Major Milestones in Corrective Actions (C-Completed)

Date	Milestones
C	Appoint DoD TAV Joint Task Force
C	Establish a JTAV Executive Agent
C	Establish a JTAV Office
C	Prepare JTAV Implementation Plan
C	Identify JTAV Priorities and Provide Milestone Schedule for JTAV Implementation
C	Demonstrate JTAV In-Theater Capability at Joint Warrior Interoperability Demonstration 95
C	Demonstrate JTAV In-Theater Capability at Cobra Gold 96
C	Field JTAV In-Theater to U.S. European Command
C	Finalize Business Rules for Interservice Visibility of Reparable Assets
C	Field JTAV In-Theater to U.S. Central Command
C	Develop a JTAV Functional Requirements Document
C	Develop a JTAV Functional “As-is” Architecture
C	Field JTAV In-Theater to U.S. Atlantic Command
C	Develop a draft JTAV Operational and Systems Architecture
C	Release JTAV In-Theater Version 2.4
C	Release JTAV Web Version 1.0

C	Field JTAV In-Theater to U.S. Pacific Command
C	Field JTAV In-Theater to U.S. Forces Korea
C	Initial Demonstration of "To Be" Architecture
C	Provide Initial Capability for Interservice Visibility of Reparable Assets
C	Provide Operational Medical Shared Data Server
C	Field Phase 1 Ammunition Asset Visibility
C	Release JTAV In-Theater Web Version 2.0
C	Field JTAV In-Theater to U.S. Southern Command
C	Field JTAV In-Theater to U.S. Special Operations Command
C	Field Phase 2 Ammunition Asset Visibility
C	Field Objective Architecture Release 1.0
C	Field Phase 3 Ammunition Asset Visibility
C	Field Objective Architecture Release 2.0
C	Complete Development of Visibility of Assets In-Theater
C	Verification of completion of milestones. At the time the Department identified TAV as a systemic weakness, the capability to share logistics information on the location, condition, quantity, and availability of assets within and between Components and the CINCs did not exist. Since that time, the Department has made great strides in providing a capability for asset visibility across the Components for the CINC and Joint Task Force Commander by linking databases across the Department. The JTAV application includes visibility of subsistence, construction, major end items, unit equipment, repair parts, fuel, ammunition, medical materiel and blood in addition to personnel and requisition tracking. A JTAV Acquisition Integrated Process Team has been established to bring the application under strict management discipline. As a result, the Department decided to extend funding through FY 2005--evidence of the commitment to provide this critical application. Implementation of this application and completion of all of the associated milestones closes this systemic control weakness.

Office of the Secretary of Defense Functional Proponent Point of Contact:

Ms. Debra Bennett
Office of the Deputy Under Secretary of Defense (Logistics)
Pentagon, Room 3B724
Washington, D.C. 20301
Telephone: (703) 692-6031 FAX: (703) 697-3428
E-mail: bennetds@acq.osd.mil

Related Initiatives

A major control issue/systemic weakness is a statement of a broadly defined management control deficiency of a Department-wide nature. Individual DoD Components have reported on efforts to correct management control weaknesses that are supportive of departmental systemic initiatives. These Component weaknesses are listed below for information purposes. The list identifies the reporting DoD Component and, within each Component, the status of those weaknesses (either unresolved or resolved during FY 2000). Furthermore, Volume II of the Annual Statement of Assurance contains additional weaknesses that have no specific correlation to reported systemic weaknesses, but have been identified by the DoD Components in order to achieve full compliance with management control guidelines.

Department of the Army

Unresolved:

Equipment In-Transit Visibility

Department of the Navy

Unresolved:

Asset Visibility of In-Transit Inventory

U. S. Transportation Command

Unresolved:

Asset Intransit Visibility

Management of Unexploded Ordnance

Statement of the Problem: The Department has an extensive test and training range complex. Ranges and their associated infrastructure are finite resources that DoD Components must maintain properly to ensure they support sustainable, safe, and efficient testing and training operations into the foreseeable future. The Department also has a significant liability at closed ranges, ranges being transferred through the Base Realignment and Closure (BRAC) program process, and ranges on formerly used Defense sites (FUDs). Unexploded ordnance (UXO) and explosives residue can present a hazard to those personnel conducting tests or training in range areas. There also exists either the potential for changes in range use (e.g., from test range to maintenance area) or the possibility that the Department might transfer a range for public, private, or other agency use (e.g., under the BRAC). In addition to safety concerns, there is uncertainty regarding the environmental impact of the use of munitions on ranges---both from munitions functioning and from leaving UXO (including munitions that low-order detonated) on ranges over long periods of time.

Practicing sustainable use of test and training ranges is essential to ensure that the Department has the capacity—now and in the future—to fulfill its mission. There are increasing regulatory and public interest pressures threatening the Department's use of its ranges due to concerns about cleanup of UXO and other related contaminants. The Department and its Components have various policies that address UXO only from a safety standpoint. The Department, however, currently lacks policies addressing Component responsibility for environmental and explosives safety management of active and inactive (AI) ranges and cleanup of UXO at closed, transferred, and transferring (CTT) ranges. These policies are essential to ensure a balance between readiness, safety, and the environment by determining how the government cleans up UXO and other environmental contaminants on ranges.

With the exception of UXO cleanup on FUDS, the Military Departments do not account for UXO clearance and cleanup in the DoD Planning, Programming, and Budgeting System (PPBS). The current rate of funding for UXO cleanup on FUDS is inadequate to meet the Department's responsibility to protect human health and safety at properties that are no longer under DoD control.

Source of Identification: Defense Science Board Task Force on UXO draft report, April 1998; Department of the Army's FY 1998 Annual Statement of Assurance that cited a material weakness, entitled "Management of Unexploded Ordnance;" and numerous reports of the OIG, DoD.

Potential Impact of the Problem: If the Department fails effectively to address UXO and other environmental contamination of AI and CTT ranges there could be: (1) unacceptable exposure to UXO, possibly resulting in injuries or death to DoD and non-DoD personnel, and (2) continued uncertainty regarding environmental impacts of munitions use on ranges. In response, external regulatory and public interests will attempt to: (1) control how the government regulates the Department's use of its ranges to test weapons and train forces, (2) affect the Department's ability to renew or acquire additional land withdrawals for use as ranges, and (3) direct stringent,

very costly cleanup requirements at CTT ranges.

Furthermore, realistic test and training is critical to ensuring the Components can train as they fight. On June 20, 2000, the Military Departments briefed DoD's Senior Readiness Oversight Council (SROC) on encroachment and other range sustainability issues. Based on that briefing, SROC members reached consensus that ensuring range sustainability on Defense ranges and training centers is a serious and growing challenge to readiness. The SROC also determined that the Department needs a comprehensive and coordinated approach to address range sustainability issues. The Department identified eight encroachment issues as part of the SROC process, including the issue of UXO and other constituents. Finalizing the Munitions Action Plan (MAP) and implementing MAP recommendations are key aspects to the broader UXO issue.

Possible Solutions: The Department must issue: (1) policy for cleanup of CTT ranges within and outside the United States and (2) PPBS guidance, e.g., Defense Planning Guidance (DPG) goals and Program Objective Memorandum (POM) Preparation Instructions (PPI), to ensure that the Military Departments plan, program, and budget appropriate funding for assessments of environmental contamination and UXO clearance/cleanup on ranges. The Military Departments should institutionalize assessment of environmental contamination and management of UXO clearance/cleanup on ranges in their Operations and Maintenance (O&M) budgets.

Major Milestones in Corrective Actions: (C = Completed)

Completed Milestones:

Date:	Milestone:
C	Establish Operations and Environment Executive Steering Committee for Munitions (OEESCM) to coordinate UXO and other munitions issues across the Military Departments and functional areas.
C	Establish PPI to collect UXO cleanup funding data for CTT ranges.
C	Collect funding data for UXO cleanup for CTT ranges as a supplemental display in the FY 2000-2005 POM.
C	Collect FY 2001-2005 POM data for funding UXO cleanup at CTT ranges.
C	Publish DoD Directive 4715.11, "Environmental and Explosives Safety Management on Department of Defense Active and Inactive Ranges Within the United States," August 17, 1999; and DoD Directive 4715.12, "Environmental and Explosives Safety Management on Department of Defense Active and Inactive Ranges Outside the United States," August 17, 1999.

C	Ensure that the Military Departments begin efforts to establish the necessary procedures to implement their responsibilities under DoDD 4715.11 and DoDD 4715.12.

Planned Milestones (Beyond FY 2000):

12/00	Establish FY 2002-2007 PPI format for collecting funding data for sustainable AI range management efforts required by DoDD 4715.11 and DoDD 4715.12, in coordination with the USD(P&R) and the Director, Program Analysis and Evaluation (PA&E). If time constraints prevent formal collection of data in the FY 2002-2007 POM, obtain PA&E concurrence to include as a supplemental display in the POM.
01/01	Finalize Munitions Action Plan.
03/01	Ensure that the Military Departments complete efforts to establish and implement procedures to assess the environmental impact of the use of munitions on DoD ranges.
03/01	Establish language for the FY 2002-2007 DPG and PPI for sustainable AI range management efforts in coordination with the Under Secretary of Defense (Personnel & Readiness) (USD(P&R)).
05/01	Collect FY 2002-2007 POM data for funding sustainable AI range management efforts via either official format or supplemental display.
05/01	Publish DoD Directive 4715.BB, “Environmental and Explosives Safety Management Policy for Closed, Transferred, and Transferring (CTT) Ranges.”
05/01	Collect FY 2002-2007 POM data for funding sustainable AI range management efforts and UXO cleanup at CTT ranges.
05/01	Collect FY 2002-2007 POM data for funding UXO cleanup at CTT ranges.
05/01	Issue guidance to all DoD Components on establishing and maintaining complete inventories of all DoD ranges in coordination with the Deputy Under Secretary of Defense (Installations) (DUSD(I)).
06/01	Publish revised draft Range Rule for public comment.
06/01	Ensure that the Military Departments initiate inventories of AI and CTT ranges consistent with DUSD(ES)/DUSD(I) guidance.

07/01 Ensure that the Military Departments complete inventories of AI and CTT ranges consistent with DUSD(ES)/DUSD(I) guidance.

Planned Milestones (Beyond FY 2001)

10/01 Ensure that the Military Departments implement the procedures, developed in FY 2001 with funding included in their FY 2002-2007 POMs, to assess the environmental impact of the use of munitions on DoD ranges.

12/01 Ensure that the Military Departments' management plans, at the installation or responsible activity level, include planning for sustainable range use. This planning, at a minimum, will address: long-term sustainable use; management procedures; record keeping; standards; monitoring; public outreach and public participation programs, if required; technology requirements to ensure sustainable range management; integration with other installation planning processes; and resources.

02/02 Determine whether effort to promulgate a Range Rule for CTT ranges is achievable.

02/02 Ensure that the Military Departments establish procedures for range clearance operations to permit the sustainable safe use of DoD ranges for their intended purpose. In determining the frequency and degree of range clearance operations, ensure they consider, at a minimum, the safety hazards of clearance, each range's intended use, and the quantities and types of munitions expended on that range.

Office of the Secretary of Defense Functional Points of Contact:

Mr. Bruce Beard, ODUSD(ES)
Phone: (703) 604-0521
Fax: (703) 607-3124
E-mail: bruce.beard@osd.mil

Col John Selstrom, USAF, ODUSD(ES)
Phone: (703) 697-9107
Fax: (703) 695-4981
E-mail: john.selstrom@osd.mil

Related Initiatives

A major control issue/systemic weakness is a statement of a broadly defined management control deficiency of a Department-wide nature. Individual DoD Components have reported on efforts to correct management control weaknesses that are supportive of departmental systemic initiatives. These Component weaknesses are listed below for information purposes. The list identifies the reporting DoD Component and, within each Component, the status of those weaknesses (either unresolved or resolved during FY 2000). Furthermore, Volume II of the Annual Statement of Assurance contains additional weaknesses that have no specific correlation to reported systemic weaknesses, but have been identified by the DoD Components in order to achieve full compliance with management control guidelines.

Department of the Army

Unresolved:

Management of Unexploded Ordnance and Other Constituents

Information Assurance

Statement of the Problem: Over the last several years, the Department has experienced numerous computer system intrusions that have highlighted the vulnerability of information systems to information-warfare-type attack. During this time, DoD sensitive but unclassified systems and networks used to support finance, logistics, medical, procurement, personnel, and research and development activities--and other support and sustainment functions--have been probed, with some systems successfully penetrated. No classified DoD systems have been penetrated from the outside, but potential disruption from the 'trusted insider' continues to exist.

Source Identifying Weakness: Audit reports, to include OIG, DoD Report Number 99-069, "Summary of Audit Results--DoD Information Assurance Challenges," dated January 22, 1999; and GAO Final Report, GAO/AIMD-99-107, "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk."

Potential Impact of the Problem: DoD dependence on information systems makes information assurance (IA) a critical readiness issue. It also is critical on a national level as systems and networks of the Global Information Grid (GIG) develop and integrate into the larger National Information Infrastructure (NII). This problem was identified in 1998 and, although many corrective actions have been implemented, intrusions continue to occur.

Possible Solutions: Improvement in IA is top priority across the entire Department, including all Components. The Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD(C3I)) monitors progress through feedback obtained during DoD Chief Information Officer (CIO) Executive Board meetings; periodic updates received as a result of previous audits; extensive use of OIG,DoD teams that have been trained to follow-up on IA-related areas; staff visits by senior OASD(C3I) personnel to the CINCs and Components; follow-up reporting generated through Information Assurance Vulnerability Alert (IAVA) process. The Department has instituted many parallel initiatives to address these areas. In this regard, the Department is increasing each of the following:

- Number of personnel trained and certified in information technology (IT) security (users and system administrators) for all levels of classification; number of intrusion detection systems deployed across DoD networks;
- Number of DoD Public Key Infrastructure (PKI) certificates issued; number of PKI Local Registration Authorities and Certificate Authorities established;
- Number of programs receiving Defense Information Technology Security, Certification and Accreditation Process (DITSCAP) approval;
- Number of products certified in National Information Assurance Partnership (NIAP) under Common Criteria evaluations;
- "Red Team" exercises and evaluations;
- Deployment of a cohesive and coordinated attack sensing and warning network; and
- Thorough security vulnerability assessments.

Major Milestones in Corrective Actions (C = Completed)

To date, the Department has implemented several IA initiatives to prevent unauthorized access to defense networks, systems, and data. These are described below.

Date	Milestone
C	Implement and improve the IAVA process to alert forces of security vulnerabilities and ensure corrective actions are completed.
C	Implement the Deputy Secretary of Defense Personnel Attestation Policy Certificate program to renew and affirm commitment to protecting information.
C	Develop and publish DoD policy guidance for PKI implementation.
C	Review DoD Web pages and removes information that reveals unclassified information that could by itself, or combined with other unclassified materials, reveal vital operational capabilities or vulnerabilities.
C	Influence DoD research and development investment for IT and IA related projects.
C	Complete IA/IT Integrated Process Team (IPT) and recommend actions to DoD senior officials with respect to improving training and retention of critical skills required of personnel operating and maintaining IT systems.
C	Revise policy for the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) to control and monitor access between the DoD and the Internet.
C	Complete PKI Implementation Plan, PKI Roadmap, and PKI Certificate Policy to establish firm milestones and technical requirements to implement PKI infrastructure and operations.
C	Develop Attack Sensing and Warning Strategy across the GIG to allow Cohesive response and coordination when intrusions occur.

C	Develop new policy establishing a balanced risk management approach to achieve required levels of IA for all information systems supporting DoD operational readiness and mission effectiveness. These issuances will replace DoD Directive (DoDD) 5200.28, "Security Requirements for Automated Information Systems (AIS)," the accompanying manual, and DoDD 5200.5, "Communications Security."
C	Reach Full Operational Capability (FOC) for DoD Computer Forensics Training Center and DoD Forensics Lab to improve the Department's capability to analyze computer intrusion events.

Planned Milestones (FY 2001)

11/00	Complete the directive and instruction on computer network defense.
12/00	Install a minimum of Class 3 server certificates, issued by DoD PKI, on all private (not publicly accessible) web servers.
01/01	Encourage DoD Components to give preference to National Information Assurance Partnership (NIAP) evaluated commercial IA products for national security systems.
Ongoing	Subject DoD business processes to robust functional process improvements to include IA that will provide needed system protections.

Planned Milestones (Beyond FY2001)

12/01	Deploy the capability to issue PKI Class 3 certificates to every DoD organization.
.	
07/02	Mandate (hence forward) that only NIAP approved commercial IA products be purchased for national security systems.
10/02	Issue a Class 3 certificate or higher to all DoD users and ensure that electronic mail is protected by digital signature. All private DoD and DoD-interest web servers will require client identification and authentication using Class 3 certificates.
Ongoing	Continue OASD(C3I) efforts to emphasize the importance of computer security throughout the Department. This includes efforts to: (1) accelerate the correction of computer security weaknesses reported in the Annual Statement of Assurance or audit reports, (2) ensure that appropriate computer security policies and procedures have been issued,

(3) strongly enforce computer security policies, and (4) test their capabilities on a regular basis to identify exposures and vulnerabilities, and eliminate them.

Office of the Secretary of Defense Functional Proponent Point of Contact:

Mr. Richard C. Schaeffer, Jr.
Director, Infrastructure & Information Assurance
Office of the Deputy Assistant Secretary of Defense
(Security and Information Operations)
Telephone: 703-695-8705

Related Initiatives

A major control issue/systemic weakness is a statement of a broadly defined management control deficiency of a Department-wide nature. Individual DoD Components have reported on efforts to correct management control weaknesses that are supportive of Departmental systemic initiatives. These Component weaknesses are listed below for information purposes. The list identifies the reporting DoD Component and, within each Component, the status of those weaknesses (either unresolved or resolved during FY 2000). Furthermore, Volume II of the Annual Statement of Assurance contains additional weaknesses that have no specific correlation to reported systemic weaknesses, but have been identified by the DoD Components in order to achieve full compliance with management control guidelines.

Department of the Army

Unresolved:

Information Systems Security

Department of the Navy

Unresolved:

Navy's Military Personnel Records System Needs Replacement

Department of the Air Force

Unresolved:

Information Technology Operations

Computer and Information Security

Defense Commissary Agency

Resolved:

Automated Information System Firewalls

DFAS

Unresolved:

Project Bankroll-Fraud Potential

Project Bankroll-Unauthorized Access Security Controls of Non-DFAS User Networks

Data Encryption Over the NIPRNet

U. S. Central Command

Unresolved:

Automated Information Systems Security (Training) in the U. S. Central Command

Automated Information Systems Security (Acquisition) in the U.S. Central Command

U. S. Strategic Command

Resolved:

Top Secret Control Program

Year 2000 Computer Problem

Statement of the Problem: The world's inventory of computer systems included extensive hardware and software that process dates using two digits. Each system needed to be examined for its ability to use date-related information throughout the transition from calendar year 1999 to 2000. The scope, magnitude, and complexity of the problem exceeded the time and resources available to fix all date-related errors prior to January 1, 2000. The Department, along with other organizations worldwide, prioritized its remediation and replacement efforts in keeping with it own mission priorities.

Source of the Identification: Executive Order; OMB; the Congress; GAO; OIG,DoD; and DoD senior management.

Potential Impact of the Problem: Any computer system that processes date-related information potentially was affected by the Year 2000 (Y2K) computer problem. The use of computer systems, for data processing and electronic control of mechanical devices, appliances, and infrastructure components, is pervasive. Consequently, the Y2K problem could affect the operations of government, manufacturing, commerce, transportation, communications, and day-to-day functioning of cities and nations. The Y2K problem also had the potential for causing corruption of data used in computer systems, which, if undiscovered, could cause delayed deterioration or errors in data processing systems.

Possible Solutions: The Department addressed the Y2K problem from the perspective of its impact on national security. The major components of the process were:

- Declaring Y2K to be a threat to national security and focusing senior leadership efforts by the Secretary of Defense and Deputy Secretary of Defense.
- Oversight of Y2K efforts by the Deputy Secretary of Defense in monthly Y2K Steering Committee meetings.
- Supporting the actions of the President's Council on Year 2000 Conversion.
- Operational evaluation of DoD mission capabilities in a Y2K environment.
- Remediation, replacement, or retirement of DoD systems to achieve Y2K compliance.

Major Milestones in Corrective Actions (C = Completed)

Completed Milestones

Date	Milestone
C	Complete Awareness Phase.
C	Complete Y2K Assessment Phase (Progress on phases reported to OMB monthly and quarterly).

C	Complete Y2K Renovation Phase.
C	Complete interface agreements between all DoD mission critical systems.
C	Test plans developed for DoD major functional areas.
C	Complete quarterly report to OMB (due in February, May, August, and November).
C	Complete Y2K Validation Phase.
C	Complete Y2K Implementation Phase.
C	Complete reporting of systems Y2K compliance status by phase to OMB.
C	Complete Monthly DoD Y2K Steering Committee meetings chaired by Deputy Secretary of Defense and attended by the Chair, President's Council on Year 2000 Conversion, OMB, GAO, and congressional staff.
C	Complete testing of all system contingency plans.
C	Complete operational evaluations of Y2K compliance.
C	Complete functional end-to-end evaluations.
C	Complete systems Y2K remediation and implementation.
C	Complete DoD Y2K Transition Period.
Note:	With Y2K conversion and the Y2K transition period activities complete, the ASD(C3I) Y2K Office was disestablished in conjunction with the DASD(DCIO) reorganization on February 28, 2000.

Planned Milestones (Beyond FY 2001): Not applicable

Office of the Secretary of Defense Functional Proponent Point of Contact:

Ms. Sandy Rogers
Office of the Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)
Telephone: (703) 602-0980, Ext. 121

Related Initiatives

A major control issue/systemic weakness is a statement of a broadly defined management control deficiency of a Department-wide nature. Individual DoD Components have reported on efforts to correct management control weaknesses that are supportive of departmental systemic initiatives. These Component weaknesses are listed below for information purposes. The list identifies the reporting DoD Component and, within each Component, the status of those weaknesses (either unresolved or resolved during FY 2000). In addition to the DoD Components specified below, efforts are underway throughout the Department to ensure proper computer system

operations beyond 1999. Furthermore, Volume II of the Annual Statement of Assurance contains additional weaknesses that have no specific correlation to reported systemic weaknesses, but have been identified by the DoD Components in order to achieve full compliance with management control guidelines.

Department of the Army

Resolved:

Year 2000 Computer Problem

Department of the Air Force

Resolved:

Year 2000 Software Logic Problem

Defense Commissary Agency

Resolved:

Y2K Noncompliance

Defense Financial and Accounting Service

Resolved:

Conformity of DFAS Systems to Year 2000 Requirements

Defense Threat Reduction Agency

Resolved:

Year 2000 Computer Problems

Special Operations Command

Resolved:

Year 2000 Computer Problem

Personnel Security Investigations Program

Statement of the Problem: The GAO found that personnel security investigations within the Department were not being conducted in a timely manner and many of the investigations were reportedly not meeting required national investigative standards for coverage.

Source of Identification: GAO Report No. NSIAD-00-12, "DOD PERSONNEL: Inadequate Personnel Security Investigations Pose National Security Risks," October 27, 1999, and subsequent reviews.

Potential Impact of the Problem: The purpose of the personnel security investigations (PSI) program is to determine whether an individual should be: (1) granted access to classified information, (2) accessed or retained in military service, or (3) employed in a sensitive position. Thus, it is important that these investigations be conducted in a thorough and timely manner. If concerns are not resolved, there may be a potential risk to the DoD personnel security program, as well as to the protection of classified and other sensitive information vital to the accomplishment of DoD core missions.

Possible Solutions: In the previous annual assurance statement, the Defense Security Service (DSS) identified the Personnel Security Investigations Program as being a material weakness and provided an action plan that addressed corrective actions needed to bring the program into compliance with performance expectations and with existing security policies. The plan provides milestones for: improving performance of the automated Case Control Management System (CCMS), providing additional training to existing investigative agents, ensuring that investigative procedures are in compliance with existing policy directives, recruiting and training additional agents, establishing an augmentation management office, and establishing investigative standards for contractors and reserve components to achieve existing security policy objectives.

Major Milestones in Corrective Actions: (C = Competed)

At the time the plan was established, the DSS had implemented several initiatives to improve the quality and timeliness of its Personnel Security Investigations products, as identified below:

Date	Milestone
C	Evaluate investigative policy against federal standards.
C	Review and rewrite investigations manual (DSSM 20-1).
C	Develop plan to evaluate and remedy backlog of Periodic Reinvestigations (PRs) within the Department.
C	Establish a plan for the DSS Standards and Quality Function.

- C Establish Program Management Office operated by the Air Force to provide expert support for infrastructure enhancements, development and acquisitions, to get current automation system to a stable operation.

- C Deploy a new Case Control Management System (CCMS) release, to reduce the number of workflow user tasks, thus increasing the system throughput.

- C Establish Operational Standards and Quality Council (first meeting on October 13, 1999).

- C Develop formal training on federal standards for new case analysts. Implement curriculum at DSS Academy/Personnel Investigations Center.

- C Establish, staff, and operate DSS Offices of Standards and Evaluation (S&E) and Quality Management (SQM). Develop and promulgate DSS Quality Management Plan (QMP).

- C Implement curriculum review to ensure quality initial training to all new investigative personnel.

- C Implement curriculum review to provide quality continuing education to all investigative personnel. Upgrade and improve training. Integrate new manual/ standards within the revised Personnel Security Investigations curriculum that includes the new agent mentoring program, basic agent course, and continuing education products for the existing workforce.

- C Implement automation infrastructure enhancement actions pertaining to CCMS, including upgraded hardware, query performance improvement, increased system availability, and ensuring interface abilities with FBI and OPM SII.

- C Develop Quality Plan that includes first-line supervisory review, ensures high-quality products, Personnel Investigations Center (PIC) quality review, and measures to evaluate returned work.

- C Stand-up operational Standards and Evaluation Functions in field, with the DSS Standards and Evaluation (Stan/Eval) Personnel Security Program fully functional.

- C Work with adjudicative community, addressing the whole person concept and issuing a related DSS Operating Instruction.

- C Ensure effective communication with field investigators, including having a smaller span of control at both the first and second level of management, which provides the opportunity for more frequent and direct contact with the field investigators and other personnel assigned to the field offices.

C	Implement hiring plan to hire highly qualified investigative personnel; establish basic skill level requirements for investigative personnel.
C	Initiate work with services to obtain overseas coverage, including actions by the Operational Standards and Quality Council (OSQC) to set up a working group to explore the options available to meet overseas coverage requirements.
C	Develop and commence implementation of a evaluation system plan to assess training needs and to measure effectiveness, including end of course evaluations for every course and formal requirement and validation of Personnel Security curriculum by an external customer stakeholder panel.

Planned Milestones (FY 2001)

12/00	As part of the evaluation of training needs and measurement of training effectiveness, implement -- DSS core process quality data collection -- Standards compliance data collection and training for individual reinvestigation in the security reinvestigation process -- Standards compliance data collection and training for Field Agents in PSI -- Standards compliance data collection and training for Case Analysts in PSI
03/01	Develop a four-phased training evaluation system by the DSS Academy. Development will encompass five basic areas: -- Assess the current training evaluation approach, procedures, including an identification of the underlying evaluation questions -- Develop a strategy for gathering training evaluation data. Training evaluation data is defined as: Student pretesting, in-course testing, posttesting, and course and instructor evaluation; and supervisory evaluation of training effectiveness. -- Explore and recommend reporting options -- Develop evaluation methodology and implementation plan, to include the integration of system data into existing Academy Information Management Systems -- Develop a long-term data management strategy
09/01	Complete implementation of near-term infrastructure enhancement actions pertaining to CCMS (e.g., archiving information to reduce workload; upgrade of Oracle to newer release; workflow process optimization; application optimization; subsystem separation to ease processing loads; electronic fingerprint card project; interface with the Joint Personnel Adjudication System; and on-line access for the Central Adjudication Facilities.

Planned milestones (Beyond FY 2001)

Ongoing	Implement improved internal automation capabilities to support DSS processes.
Ongoing	Pursue long-term automation infrastructure enhancement actions relating to CCMS (e.g., workflow enhancements or replacement; database engine enhancements; and additional user functionality).
Ongoing	Continuing education/training curriculum improvements are being addressed in the overall curriculum review for both programs and development is being initiated as resources are made available.

Office of the Secretary of Defense Functional Proponent Point of Contact:

Mr. Pete Nelson
Office of the Assistant Secretary of Defense
Command, Control, Communications and Intelligence
Telephone: (703) 697-3969

Related Initiatives

A major control issue/systemic weakness is a statement of a broadly defined management control deficiency of a Department-wide nature. Individual DoD Components have reported on efforts to correct management control weaknesses that are supportive of departmental systemic initiatives. These Component weaknesses are listed below for information purposes. The list identifies the reporting DoD Component and, within each Component, the status of those weaknesses (either unresolved or resolved during FY 2000).

Defense Security Service

Unresolved:

Personnel Security Investigations Program

CONCLUSION

The information provided in this Department of Defense Annual Statement of Assurance focuses on complying with the requirements of the FMFIA and OMB Circular A-123, "Management Accountability and Control." The narratives contained in this report reflect continuing improvement in the status of the systemic control weaknesses since last reported in the FY 1999 Annual Statement of Assurance. The Volume I presentation provides, at a glance, the status of the most significant internal control issues in the Department of Defense.